ABSTRACT

Methods, systems, and arrangements enable increased security for a processor, including by implementing block encryption. The block may include multiple instructions and/or operations to be executed by the processor. The block may also include multiple bytes that are read into the processor byte by byte. Once a block-wide encrypted buffer has been filled from an external memory source, the block may be decrypted using an encryption algorithm (e.g., the Data Encryption Standard (DES), the triple DES, etc.), and the decrypted block may be forwarded to a decrypted buffer. The decrypted block may thereafter be moved into a cache, which may optionally be organized into an equivalent block width (e.g., for each way of a multi-way cache). Therefore, when a processing core/instruction decoder needs a new instruction, it may retrieve one from the cache, directly from the decrypted buffer, or from external memory (e.g., after undergoing decryption).